National Infrastructure Protection Center CyberNotes

Issue #2000-07 *April 12, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 24 and April 5, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[1]	Forums 2.x	A security vulnerability exists which allows users to view and post to secure discussion threads via unsecured conferences and/or through e-mail.	Patch available at: http://download.allaire.com/patches/ASB00-07forumfix.zip The template files were created to replace the existing files on your system. It is recommended you back up your existing data before over-writing or replacing any files. You will also need to modify these files to reflect any personal coding changes you have made to your existing Forums installation.	Allaire Forums "RightAccessAll Forums" Vulnerability	High	Bug discussed in newsgroups and websites.

[1] Allaire Secure Advisory, ASB00-06, April 3, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
AnalogX[2]	SimpleServer WWW 1.0.3, 1.0.4	The request processing procedure contains a buffer overflow vulnerability.	Upgrade to Simple Server WWW 1.04 located at: http://www.analogx.com/files/sswwwi.exe	SimpleServer WWW 1.03 Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
BinTec Communica-tions[3]	ISDN router BIANCA/BRICK-XL; BIANCA/BRICK-XS;	A malicious user is able to gain the management accounts passwords, which are the same as the SNMP community names, by using SNMP brute-force-techniques. These routers also offer the following services which can be abused easily: dialing out and getting full line access via a CAPI interface; or a debugging interface which gives you all information which is sent over the BRI-lines.	Workarounds: Disable: (admin.biboAdmSnmpPort=0) (admin.biboAdmSnmpTrapPort=0) RCAPI: disable or password protect (admin.biboAdmCapiTcpPort=0) BrickTrace: disable (admin.biboAdmTraceTcpPort=0)	BinTec Router Security and Privacy Weakness	Medium	Bug discussed in newsgroups and websites.
Citrix[4]	MetaFrame for Unix 1.0; MetaFrame for Windows 2000 1.8 and earlier; MetaFrame for Windows NT 4.0 TSE 1.8 and earlier; WinFrame for Windows NT 3.5 1.8	A vulnerability exists in the ICA (Independent Computing Architecture) protocol which could allow a malicious user to crack the encryption scheme used to protect user authentication, as well as perform more advanced attacks such as a man-in-the-middle attack or even a session hijacking.	No workaround or patch available. However Citrix offers a product called SecureISA for use with WinFrame servers and clients, which supports Diffie-Helman key exchange and RC5 transport encryption. More information on this can be found at: Http://www.citrix.com/products/sica/	ICA Weak Encryption	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Cobalt Networks[5]	RaQ 2.0, 3.0	A vulnerability exists which could allow remote malicious users to view the contents of an .htaccess file contained within a public website. This will likely affect other Cobalt products. This could lead to unauthorized retrieval of username and password information for restricted portions of a website hosted on the server.	Patch available at: Cobalt RaQ 2.0: ftp://ftp.cobaltnet.com/pub/experimental/security/apache/RaQ2-All-Security-Point-2.97.pkg RaQ 3: ftp://ftp.cobaltnet.com/pub/experimental/security/apache/RaQ3-All-Security-Point-2.4.pkg	Cobalt Raq Apache .htaccess Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[2] Bugtraq, March 25, 2000.
[3] TESO Security Advisory, 2000/03/30, April 1, 2000.
[4] Bugtraq, March 29, 2000.
[5] Cobalt Networks Security Advisory, 03.31.2000, March 31 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
GeoCel International[6]	WindMail 3.0	Multiple vulnerabilities exist which could allow a remote malicious user to e-mail system files to an e-mail address and possibly execute command-line commands.	Windmail was not designed for interactive CGI use; you should remove it from any web-accessible directory.	GeoCel WindMail Remote File Read	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[7]	HP-UX 11.4; VirtualVault 3.50	A vulnerability exists which allows data to be delivered via a network interface to unprivileged processes if multiple IP addresses are assigned to the interface.	No workaround or patch available at time of publishing.	HP VirtualVault Aliased IP Addresses	Medium	Bug discussed in newsgroups and websites.
IBM[8]	IBMHSSSB 1.0	A vulnerability exists in the /usr/bin/ikeyman shell script, which could allow an unprivileged user to use ikeyman to run commands of their choice as root.	No workaround or patch available at time of publishing. Temporary workaround: Remove either the SUID bit or the reference to the existing classpath from /usr/bin/ikeyman	IBM Ikeyman Java Class Creation Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Imatix[9]	Xitami Webserver	Several buffer overflow vulnerabilities exist which could allow a malicious user to cause a Denial of Service.	Version 2.4d7 fixes this vulnerability.	Xitami Webserver Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Ipswitch[10]	Imail 5.0, 5.0.5-5.0.8, 6.0- 6.2	A Denial of Service vulnerability exists in the implementation of IMail's authentication scheme. This problem has been confirmed to be only with Eudora at this time.	Workaround can be found in the IpSwitch Knowledge Base article at: http://support.ipswitch.com/kb/IM-20000208-DM02.htm	IMail Server Authentication Denial of Service	Low	Bug discussed in newsgroups and websites.
Michael A. Gumienny[11]	FCheck 2.7.45	Because it calls system() with a scalar argument, a malicious user can cause it to execute programs by creating files with shell metacharacters in their names.	Unofficial patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/fcheck.patch	FCheck Shell Metacharacter Filename	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[6] Security Alert Consensus Number 038 (00.14), March 30, 2000.
[7] HP Security Advisory, HPSBUX0004-112, April 4, 2000.
[8] Bugtraq, April 5, 2000.
[9] SecurityFocus, March 29, 2000.
[10] Bugtraq, April 5, 2000.
[11] Bugtraq, March 31, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[12]	Excel 97/2000	A security vulnerability exists which could allow a malicious user to trick a user into executing a macro without generating the expected security warning.	Patch available at: Microsoft Excel 97: http://www.officeupdate.com/isapi/gooffupd.asp?TARGET=/downloaditems/xl8p9pkg.exe This patch requires Office 97 Service Release 2. Microsoft Excel 2000: http://download.microsoft.com/download/office2000pro/o2ksr1/2000/WIN98/EN-US/o2ksr1.exe The vulnerability is eliminated with this Office 2000 Service Release 1 (SR-1) Update.	Microsoft Excel XML	Low	Bug discussed in newsgroups and websites.
Microsoft[13]	Commercial Internet System 2.0, 2.5; IIS 4.0, 5.0; Proxy Server 2.0; Site Server 3.0 Commerce Edition; Site Server 3.0; Commercial Internet System 2.0; BackOffice 4.0, 4.5	A security vulnerability exists in the Internet Information Server and products based on it, which could let a remote malicious user download the source code for web files that are located on UNC shares mounted on a virtual web directory.	Patch available at: Internet Information Server 4.0 Intel: http://www.microsoft.com/downloads/release.asp?ReleaseID=18900 Alpha: http://www.microsoft.com/downloads/release.asp?ReleaseID=18901 Internet Information Server 5.0 http://www.microsoft.com/downloads/release.asp?ReleaseID=19982 **NOTE:** Proxy Server, Site Server, Site Server Commerce Edition and Microsoft Commercial Internet System run atop IIS. Customers using these products should apply the patch appropriate for the version of IIS they are running.	Microsoft Virtualized UNC Share	Medium	Bug discussed in newsgroups and websites.
Microsoft[14]	Index Server 2.0	A security vulnerability in the Index Server has been found. This vulnerability affects any web site running IIS 4 or 5 with Index Server even if no .htw files exist on the file system. A malicious user could view the source code of an ASP page or other file such as the gobal.asa, which contain sensitive information such as user Ids and passwords, and database source names.	Microsoft has re-released security Bulletin MS00-006 with a new patch to address this issue. Microsoft Index Server 2.0: http://download.microsoft.com/download/winntsp/Patch/MHH/NT4/EN-US/Q252463i.EXE Intel: http://download.microsoft.com/download/winntsp/Patch/MHH/ALPHA/EN-US/Q252463a.EXE	MS Index Server '%20' ASP Source Disclosure Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[12] Microsoft Security Bulletin, MS00-022, April 3, 2000
[13] Microsoft Security Advisory, MS00-019, March 30, 2000.
[14] Cerberus Information Security Advisory, CISADV000330, March 31, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[15]	Windows NT 4.0, 2000; Windows NT Terminal Server	A security vulnerability exists in the TCP/IP Printing Services, which could allow a malicious user to disrupt printing services.	Patches available at: Windows NT 4.0: http://download.microsoft.com/download/winntsp/Patch/Q257870/NT4/EN-US/Q257870i.EXE Intel: http://download.microsoft.com/download/winntsp/Patch/Q257870/ALPHA/EN-US/Q257870a.EXE Windows NT 2000.0: http://download.microsoft.com/download/win2000platform/Patch/Q257870/NT5/EN-US/Q257870_W2K_SP1_x86_en.EXE	TCP/IP Printing Service Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Linux Vendors[16] ***RedHat releases patches[17]***	**Michael Sandrof IrcII 4.4-7 for S.u.S.E. Linux 6.3; RedHat Linux 6.1 i386**	**A buffer overflow exists in the DCC chat code that allows a remote malicious user to execute arbitrary code on a client's system.**	**Upgrade to IrcII version 4.4M: ftp://ircftp.au.eterna.com.au/pub/IrcII/ircii-4.4M.tar.gz** ***Patches available at: (Please choose the proper version, [4.2, 5.2, 6.2] and architecture for your system)*** *ftp://updates.redhat.com/4.2/i386/ircii-4.4M-0.4.2.i386.rpm*	**IrcII DCC Chat Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Multiple Vendors[18]	Linux 2.1, 2.2, 2.2pre potato Linux kernel 2.2.10, 2.2.12, 2.2.14; Linux 6.0, 6.1, 6.2	A vulnerability exists in the IP Masquerading kernel code, which could allow a malicious user to rewrite the UDP masquerading entries, making it possible for UDP packets to be routed back to the internal machine.	No workaround or patch available at time of publishing.	Linux Kernel IP Masquerading	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[19]	Linux 2.2.12, 2.2.14, 2.3.99-pre2	The Linux kernel is vulnerable to a Denial of Service attack due to improper handling of Unix domain sockets.	No workaround or patch available at time of publishing.	Linux Domain Socket Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
NBase-Xyplex[20]	EdgeBlaster MultiFunction WAN Access Router	A Denial of Service vulnerability exists when the EdgeBlaster router is scanned with CyberCop for the FormMail CGI vulnerability. There is no error message or activity other than traffic halting at the router.	No workaround or patch available at time of publishing.	EdgeBlaster Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[15] Microsoft Security Advisory, MS00-021, March 30, 2000.
[16] Securiteam, March 14, 2000.
[17] Red Hat, Inc. Security Advisory, RHSA-2000:008-01, March 29, 2000.
[18] Bugtraq, March 30, 2000.
[19] Securiteam, March 24, 2000.
[20] SilverBack Security Advisory, April 5, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
PIX[21]	PIX Firewall	A Denial of Service vulnerability exists in the way the PIX Firewall handles connection state routing tables, which could enable remote malicious users to reset the entire routing table.	No workaround or patch available at time of publishing. Unofficial workaround: Map all global IPs on your external interface and then statically NAT the ports you want accessible on your DMZ through to localnet IP addresses.	PIX DMZ Denial of Service	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Real Networks[22]	RealPlayer for Windows 6.0, 7.0	An unchecked buffer overflow vulnerability exists in the 'location' field of RealPlayer, which could allow arbitrary code to be executed.	No workaround or patch available at time of publishing.	RealPlayer Location Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SGI[23]	Irix 5.2, 5.3, 5.3XFS, 6.0, 6.01, 6.01XFS, 6.1, 6.2	A vulnerability exists in the objectserver(1M) daemon which can lead to unauthorized non-privileged user accounts being created. While a patch was made available, and IRIX 6.2 systems were thought to be fixed, the patch merely prevented the creation of root accounts, and did nothing to prevent the creation of other accounts.	Patches are available at: http://support.sgi.com	Irix Objectserver Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit script has been published. This vulnerability has existed in the wild since 1997, and was well publicized.
Standard & Poor[24]	ComStock 4.2.4	ComStock is based on the RedHat 5.1 distribution, and contains many of the vulnerabilities found in the 5.1 distribution. In addition, it contains numerous accounts with weak, or nonexistent passwords.	No workaround or patch available at time of publishing.	Standard & Poor's ComStock Machine Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems[25]	Solaris 7	Four Denial of Service BIND vulnerabilities exist which could allow a remote malicious user to degrade performance and cause the system to crash.	Patch available at: http://sunsolve.sun.com/securitypatch	Solaris BIND Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[21] Securiteam, March 24, 2000.
[22] Bugtraq, April 3, 2000.
[23] SGI Security Advisory, 20000303-01-PX, March 28, 2000.
[24] Bugtraq, March 24, 2000.
[25] Sun Microsystems, Inc. Security Bulletin, #00194, March 29, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Symantec[26]	PcAnywhere 9.0	A weak encryption scheme is used to encrypt username and password transmittal, which could allow a malicious user to retrieve the usernames and passwords.	Symantec recommends implementing symmetric or public encryption with pcAnywhere. Information on this subject can be found in the following Knowledge Base Article: http://service1.symantec.com/SUPPORT/pca.nsf/pfdocs/1999022312571812	Symantec PcAnywhere Weak Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
vqSoft[27]	vqServer 1.9.9	Passwords are stored in plaintext format, which could allow a remote malicious user to gain access to the server's configuration file. This could allow him/her to overtake the server and completely compromise the operating system.	Upgrade to the latest version available at: http://www.vqSoft.com	VqServer Plaintext Password Storage	**High**	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 24 and April 5, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 29 scripts, programs, and net-news messages containing holes or exploits were identified.

[26] SecurityFocus, April 5, 2000.
[27] Securiteam, March 27, 2000.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 5, 2000	**Pca90.c**	**Exploit script for the pcAnywhere encryption vulnerability.**
April 3-5, 2000	**Nmap-2.30BETA18.tgz**	**An advanced utility for network exploration or security auditing. It supports ping scanning, many port scanning techniques, TCP/IP fingerprinting (remote OS detection), advanced host enumeration, firewall bypassing, flexible target and port specification, decoy scanning, determination of TCP sequence predictability characteristics, SunRCP scanning, reverse-identd scanning and more.**
April 3-5, 2000	Saint-2.0.1.beta2.tar.gz	A security assessment tool based on SATAN.
April 3-5, 2000	Cattscanner-0.6.tar.gz	A compilation of common networking tools rewritten into one massively configurable, portable, independent, fast package.
April 2-3, 2000	Irix-objectserver.c	Remote exploit script for the SGI Irix objectserver vulnerability.
April 2-3, 2000	Str-msqchk.c	Mh/msqchk and mh/inc demonstration local exploit for FreeBSD and BSDI.
April 2-3, 2000	Fdmn-smash.c	Fdmount local root exploit script, which has been tested on Slackware 4.0.
April 2-3, 2000	Snmpx.sh	Solaris 2.6 snmpdx remote exploit script.
April 2-3, 2000	**B0f-lin14.c**	**Script for Linux 2.2.14 and 2.3.99-pre2 domain socket Denial of Service vulnerability.**
March 30-April 1, 2000	**Rpc.AMD.FreeBSD3.2REL.tar.gz**	**FreeBSD 2.3-REL AMD remote root exploit script.**
March30-April 1, 2000	Windosprs.zip	Remote Denial of Service exploit for the heap memory problem in Windows TCP/IP Print Server.
March30-April 1, 2000	Nessus-0.99.10.tar.gz	A free up-to-date full-featured remote security scanner for Linux, BSD, Solaris and some other systems which performs over 330 remote security checks.
March 30-April 1, 2000	Natas.exe	An advanced network sniffer/packet analysis program designed for Windows 2000.
March 30-April 1, 2000	**Icadecrypt.c.txt**	**Cracks the weak hash encryption on stored Citrix ICA passwords.**
March 30-April 1, 2000	Nmap-2.12-vek.patch	Patch to NMAP 2.12 to do another type of stealth scan similar to the xmas scan, which is not currently logged by iplog and some IDS software.
March 30-April 1, 2000	**NXT-Howto.txt**	**Remote root exploit technique for Bind 8.2-8.2.2, which explains how to manipulate DNS records on a primary name server to exploit this vulnerability.**
March 27-29, 2000	**dsniff-1.7.tar.gz**	**Dsniff can now parse Microsoft SMB, Citrix ICA, Oracle SQL*Net (v2/Net8), and LDAP.**
March 27-29, 2000	Nomad-0.1.5.tar.gz	Nu-Nomad is a network-mapping program designed to automatically discover a local network, using SNMP to identify network devices and work out how they are physically connected together.
March 27-29, 2000	TBA_v1_prc.zip	Wardialer for the PalmOS platform.
March 27-29, 2000	**Position.c**	**Script which overflows the –position arg buffer in Wmcdplay.**
March 27-29, 2000	Saint-2.0.1.beta1.tar.gz	Security assessment tool based on SATAN.
March 27-29, 2000	Net-RawIP-0.09b.tar.gz	A Perl extension for easy manipulation of IP packets with an interface to libpcap.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
March 25-26, 2000	WinNessus-0.99.9.1.zip	Windows Nessus Client is an almost fully functional port of the UNIX Nessus Client and has the same look and feel.
March 25-26, 2000	**Nmap02.30BETA17.tar.gz**	**An advanced utility for network exploration or security auditing which supports ping scanning, many port scanning techniques, TCP/IP fingerprinting, advanced host enumeration, firewall bypassing, flexible target and port specification, decoy scanning, determination of TCP sequence predictability characteristics, sunRCP scanning, reverse-identd scanning and more.**
March 25-26, 2000	NSS_2000pre10-unx.tar.gz	Narrow Security Scanner 2000 (Unix/Perl) searches for 367 remote vulnerabilities and has been tested on RedHat, FreeBSD, OpenBSD, Slackware and SuSE.
March 25-26, 2000	NSS_2000pre10-win.tar.gx	Narrow Security Scanner 2000 (Windows/Perl) searches for 367 remote vulnerabilities and has been tested on Windows 95/98/NT.
March25-26, 2000	Infinity-t-3.00b.pl	The Infinity Perl/Tk Scanner features scanners for exploits, Trojans, ports, subnets, server information and protocols all in one using Perk/tk for a GUI. Also features a hex http query to avoid IDS systems.
March 25-26, 2000	Apsend.tar.gz	A TCP/IP packet sender to test firewalls and other network applications which includes a syn flood option, land Denial of Service attack, Denial of Service attack against TCPdump 3.4, and spoofing.
March 24, 2000	**State.c**	**Exploit script for the PIX DMZ Denial of Service vulnerability.**

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of description in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

DDoS/DoS:

- An increase in alteration of delegated nameserver information for domain names causing DNS-based Denial of Service.

Probes/Scans:

- **An increase from Brazil in exploits and scans to port 53 are being used against well-known vulnerabilities, the NXT overflow vulnerability, which creates the directory ADMROCKS after entry, and the BIND vulnerability.**
- An increase in scans on Port 98 (linuxconf).
- There has been an increase in probes to UDP Port 137 (NetBIOS Name Service).
- An increase in probes to port 1080/tcp (RingZero Trojan) and port 1243 (SubSeven Trojan).

- There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.

Other:
- Exploits are being used against the Irix objectserver vulnerability.
- An increase in exploitation of unprotected Windows networking shares.
- Exploits are still being used against well-know vulnerabilities, the RDS DataFactory object and Microsoft IIS web servers, which is a component of Microsoft Data Access Components (MDAC).
- Reports indicate registry objects being maliciously altered which include: point of contact information for domain names, IP address delegations, and autonomous system numbers.
- Forged email headers are being used to bypass weak registry transaction authentication mechanisms.
- There has been an increase in the recent distribution of worm variants of Melissa and PrettyPark.

Viruses

911 Worm (BAT/911-B, BAT.Chode.Worm, W95/Firkin.worm, Foreskin, BAT911, Bat/Firkin.B) (Batch File Worm): This is an Internet worm that uses DOS batch files (.BAT), to create a series of random computer Internet addresses (IP addresses) from known Internet Service Providers. It then attempts to link to any computer connected on one of these IP addresses to find an accessible computer with a shared C drive that is not password protected. Once a shared C drive is located, the worm will copy its files onto this other computer.

If the virus manages to access an accessible computer on one of these subnets, it creates subdirectories called C:\progra~1\chode, C:\progra~1\foreskin and C:\progra~1\dickhair. While copying its files to the other computer, the worm adds or modifies the following:

- Modifies C:\AUTOEXEC.BAT by adding an instruction to a batch file to attempt 911 calls using the computer modem. This modification is executed one out of every five infections.
- Adds two new programs to the Program-Startup group. ASHIELD.PIF references ASHIELD.EXE, a Win32 freeware program that hides program activities and is used in this case to hide the worm activity when it is launched. In addition NETSTAT.PIF is used to hide the netstat utility.
- Adds a VBS script file, called WINSOCK.VBS into the Program-StartUp of the infected machine. This VBS file carries the payload.
- Makes a record of the infection in a special log file in the source computer.

On the 19th of the month the virus will attempt to delete all files in the C:\windows, C:\windows\system, C:\windows\command subdirectories and in the C:\ root directory. Then, it displays two message boxes:

> "You Have Been Infected By Chode"
> "You may now turn this piece of sh#@ off!"

Irok-10000, VBS/Irok, VBS/Irok.Trojan (Executable and mIRC Virus): The virus spreads by infecting files, e-mailing itself and propagating over Internet Relay Chat (IRC). The virus creates a copy of itself named Irok.exe in the Windows System directory and a VBScript file named Irokrun.vbs in the Programs\Startup program group. This script is used to e-mail the virus to the first 60 entries in your Outlook address book.

The subject of the e-mail sent by the virus is: "I thought you might like to see this." The body of the message is: "I thought you might like this. I got it from paramount pictures website. It's a Startrek screen saver."

The virus is attached to the mail as a file named Irok.exe. When the file is run it will display white dots moving across the screen. If mIRC is installed it will also create a script.ini file in the mIRC directory.

Irok-7877 (Executable and mIRC Virus): It is a variant of the Irok-10000 virus, which spreads by infecting files, e-mailing itself and propagating over Internet Relay Chat (IRC).

W95/Caw.1416 (MS-DOS Virus): This is a memory-resident virus that infects all files with an .exe extension that are executed. It carries out two destructive actions on the infected computer. One, it eliminates the file that is opened when the clock minutes read either "0" or a multiple 8 and the other, it deletes any 16 sectors of the hard disk at random if an infected file is opened on the 7th of July.

WM97/Ethan-BV (Word 97 Macro Virus): This virus has been seen in the wild and is a variant of the WM97/Ethan Word macro virus. Whenever an infected document is opened it will alter the information in the File|Properties|Summary box.

WM97/Ethan-CK (Word 97 Macro Virus): This virus has been reported in the wild. It will change the file summary information to include:

Title = "Ethan Frome"
Author = "EW/LN/CB"
Keywords = "Ethan".

WM97/Hope-S (Word 97 Macro Virus): This virus has been reported in the wild and contains the comment "Lyrics From Smothered Hope".

W97M_ISENG.B (Aliases: ISENG.B) (Word 97 Macro Virus): This virus has been reported in the wild and infects the system whenever an infected document is opened and closed.

It deletes the existing user macros except for the ThisDocument stream and also disables the Tools|Macro option in the Menu bar. If the Tools|Macro or VewVBCode option was used or clicked it shows a message box with the following text:

"Please reinstall your Microsoft Office Program."

W97M/Melissa.0@mm (W97M/Duhalde) (Word 97 Macro Virus): This virus uses e-mail to spread and send itself to 100 users from each possible address book that exists in the system. It can also spread through any other means (floppy disks, CD-ROMs, computer networks, the Internet,... etc.).

On activation, W97M/Melissa.0@mm inserts a space where the cursor happens to be at that moment within the Word document. If any section is selected, it will be deleted on inserting the space. This only occurs when the following condition is met: Number of minutes in the system clock + 2 = Number of day (as in the system date) + 1. In addition, the virus disables the antivirus protection in the macros and the menu options that permit working with them.

W97M_SEKE.A (Aliases: SEKE.A) (Word 97 Macro Virus): This virus has been seen in the wild and replicates using its own module. When triggered, it displays messages and does not have a destructive payload.

The virus infects by copying its module to the Normal Template and to the active document upon opening and closing documents. Also, it disables virus protection and modifies the Application's user address as: "SEKE- Chicklayo ".

WM97/Service-A, WM97/NoArmy-A (Word 97 Macro Virus): This virus has been seen in the wild and is a complex polymorphic virus. It is similar to the Melissa family of viruses in that it mass mails to addresses in your Outlook address book but only those that end in .fr.

The subject line "Un peu d'aide..." and the text "Ce document (document name) vaut bien un petit coup d'oeil. J'aimerais savoir s'il correspond a ce qu'on attends de lui" is used.

The virus can also insert strings, in French, into user documents such as "Non au Service National - Qui au contrat de Travail" and "Qui a l'Emploi Qui a l'armee de metier, mais Non au service national sous contrat de travail, Non a l'absurdite."

W97M_TPPFORM (Aliases: TPPFORM , Bloodhound, W97M/Tarap, Tarap) (Word 97 Macro Virus): This virus has been reported in the wild.

This virus disables virus protection, saves normal prompt and confirms conversion options. It drops wtr.dll (which contains the values for the dialog box), wtv.frx and wind.sys (which contains the macro virus codes).

On the 15th day of the month it infects c:\AUTOEXEC.BAT by copying the original into autoexe and adding a text message to the infected autoexec.bat.

WM97/Walker-I (Word 97 macro virus): This virus has been seen in the wild and is an encrypted macro virus. The virus contains a function called Heidi. When an infected document is opened, the macro security in Word is switched off.

XM97/Divi-D (Excel 97 Macro Virus): This virus has been reported in the wild. It is a variant of the XM97/Divi-A Excel spreadsheet macro virus.

It creates a file called 874.XLS in the Excel startup directory, and will infect other spreadsheets as they are opened or closed.

X97M/VCX.A (Excel 97 Macro Virus): This virus infects Microsoft Excel 97 books (spreadsheets) when these are closed or disabled. Among the effects produced is the disabling of the antivirus infection that Excel incorporates in order to detect possible infections in the spreadsheet macros. This virus also modifies the Windows Registry in order to disable the Visual Basic editor and the antivirus protection of the Excel macros.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
Acid Shiver + lmacid	**v1.0 + 1.0Mod**	**Current Issue**
AOL Trojan		CyberNotes-2000-01
Bla	1.0-5.02	CyberNotes-2000-06
DeepThroat	v1.0 - 3.1 + Mod (Foreplay)	CyberNotes-2000-05
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
FakeFTP	Beta	CyberNotes-2000-02
Girlfriend	V1.3x (including Patch 1 & 2)	CyberNotes-2000-05
Hack`a`Tack	1.2-2000	CyberNotes-2000-06
Hack'A'tack	1.0-2000	CyberNotes-2000-01
ik97	**v1.2**	**Current Issue**
InCommand	1.0-1.4	CyberNotes-2000-01
Infector	**v1.3**	**Current Issue**
Intruder		CyberNotes-2000-01
Kuang Original	0.34	CyberNotes-2000-01
Matrix	1.4-2.0	CyberNotes-2000-01
MoSucker		CyberNotes-2000-06
NetController	**v1.08**	**Current Issue**
NetSphere	v1.0 - 1.31337	CyberNotes-2000-06
NetTrojan	1.0	CyberNotes-2000-06
Nirvana / VisualKiller	**v1.94 - 1.95**	**Current Issue**
Prayer	1.2-1.3	CyberNotes-2000-06
Setup Trojan (Sshare) +Mod Small Share		CyberNotes-2000-06
ShadowPhyre	v2.12.38 - 2.X	CyberNotes-2000-06
Softwarst		CyberNotes-2000-05
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02
SubSeven	**V1.0-1.9b, v2.1+SubStealth, v2.2b1**	**Current Issue**
Trinoo		CyberNotes-2000-05
TryIt		CyberNotes-2000-05
wCrat	v1.2b	CyberNotes-2000-05

Acid Shiver (March 26, 2000): Unlike common Trojans, which anyone on the Internet can scan for and exploit, only the person(s) who installed it or got you to install it can really use it against you. The port Acid Shiver uses are picked at random each time you connect to the Internet. When you connect (either on startup as a LAN, or when you dial to your ISP) the Trojan sends an e-mail to the creator (set within the EXE) who lists, among other information, the time, your IP and the random port.

New as of April 1999, there is a modified server called LMacid, which simply changes the registry lines and filenames.

ik97 v1.2 (March 26th, 2000): This is a keylogger, which records key presses to a file on the infected system. This Trojan is also shareware.

Infector v1.3 (March 26th, 2000): Infector does not let others control your computer. All this Trojan does is send an ICQ to a specified person, giving them your IP when you are online. This would be used mostly when you are infected with a different type of Trojan that doesn't have ICQ notify built in.

NetController v1.08 (March 26th, 2000): This is a non-English Trojan that seems to have features such as screencapture, open/close CDROM, and file transfers. Seems like another NetBus look-alike.

Nirvana / VisualKiller v1.94 - 1.95 (March 26th, 2000): This is a Trojan that has all the features of NetBus, and nothing more. It is a non-English Trojan with file transfer features, which could be used to install other Trojans or get personal information. It can also be used to erase your harddrive.

SubSeven (March 26, 2000): SubSeven was made to fill in the gaps left by NetBus. NetBus was the first 'point and click' Trojan that made it very easy for hackers to abuse an infected system.

SubSeven can do everything that NetBus can do. This includes things such as:

- File controls
  - Upload / Download
  - Move, Copy, Rename, Delete
  - Erase harddrives and other disks
  - Execute programs
- Monitoring
  - Can see your screen as you see it
  - Log any/all keypresses (even hidden passwords)
  - Open/close/move windows
  - Move mouse
- Network control
  - Can see all open connections to and from your computer
  - Can close connections
  - Can 'bounce' or relay from their system to yours, so wherever they connect it seems as if you are doing it. This is how they prevent getting caught breaking into other computer systems and get You in trouble!

The SubSeven Trojan can also be configured to inform someone when its infected computer connects to the Internet, and tells that person all the information about you that is needed to use the Trojan against you. This notification can be done over an IRC network, by ICQ, or by e-mail.

Trojan.Subseven.2.2 is a variant of the SubSeven Trojan. It is a backdoor Trojan that allows a malicious user to carry out unauthorized operations on an infected computer by means of a connection it opens with a remote machine. This latest threat is not currently found in the wild.

The beta version of Trojan.Subseven.2.2 is made up of four files: server, client, a DLL file (Icqmapi.dll) and a configuration program called "EditServer.Exe".

The EditServer.Exe program allows the malicious user to obtain data such as the victim's IP address (via ICQ, IRC, e-mail or static IP). Customized error messages can be used to trick the victim into believing that the program he/she has just run has encountered an error, when what has really happened is that they have installed the server program on their computer.

To ensure that it is run each time the infected computer is booted, Trojan.Subseven.2.2 uses the same methods as previous versions (changes to the Windows Registry, Win.ini or System.ini). It allows you to configure the communications port, passwords and the name of the server that will be installed in the C:\Windows\System directory.

Once installed on the victim machine, Trojan.Subseven.2.2 can download plugins or randomly named Internet files with DLL extensions and save them in the C:\Windows\system folder. It could allow the malicious user to access and remove confidential information through ICQ (ICQ Spy), keylogger applications or chat channels. It also makes it possible to update the server through a URL, edit the Windows registry, change Windows settings, and record sound and video images from the victim's computer. Trojan.Subseven.2.2 allows instructions to be sent in command-line format as well as through the client interface, and carries out other actions such as opening the CD-ROM tray or hiding the task bar or start button, etc.